Code 1

Coordinated Science Laboratory

UNIVERSITY OF ILLINOIS – URBANA, ILLINOIS

WEIGHT DISTRIBUTION FORMULA FOR SOME CLASS OF CYCLIC CODES

Tadao Kasami

REPORT R-285

APRIL, 1966

This work was supported in part by the Joint Services Electronics Program (U. S. Army, U. S. Navy, and U. S. Air Force) under Contract No. DA 28 043 AMC 00073(E), and in part by the National Science Foundation under Grant NSF GK-690, and in part by the Air Force Cambridge Research Laboratories under Contract AF 19(628)4379.

WEIGHT DISTRIBUTION FORMULA FOR SOME CLASS OF CYCLIC CODES

Tadao Kasami

Abstract

Let $h_1(X)$ and $h_2(X)$ be different irreducible polynomials such that $h_1(\alpha^{-2^h-1}) = 0$ for some $h (0 < h < m)$ and $h_2(\alpha^{-1}) = 0$, α being a primitive element of $GF(2^m)$. This paper presents the weight distribution formula of the code of length 2^m-1 generated by $(X^{2^m-1} - 1)/(h_1(X)h_2(X))$ for any m and h. Some applications to the cross-correlation problem between two different maximum length sequences are presented.

1. Introduction

W. W. Peterson [1] calculated a number of weight distributions for BCH codes of lengths 63 to 1023 and their dual codes by digital computation. He observed that some BCH codes with large t for a given m ($5 \leq m \leq 10$) have a very simple structure of weight distribution. The result presented here is a theoretical development of his observation.

Let C be a cyclic code of length 2^m-1. The extended code of C is the code with an overall parity check added to C as the first digit. The first symbol in a code vector is numbered 0, and for $i > 1$ the i-th digit is numbered α^{i-2}, α being a primitive element of $GF(2^m)$. Now for $a(\neq 0)$ and $b \in GF(2^m)$ and for a code vector v of the extended code, permute the symbol in position X to position $aX + b$. Then, the resulting vector is denoted by $\pi_{ab}v$. W. W. Peterson [1] proved that the extended codes of BCH codes are invariant under doubly transitive group of permutations $\pi = \{\pi_{ab} | a(\neq 0), b \in GF(2^m)\}$. This paper presents the weight distribution formula for a class of cyclic codes of length 2^m-1 whose extended codes are invariant under π.

Let $g_1(X)$ and $g_2(X)$ be different irreducible polynomials such that

(1) $g_1(\alpha^{2^h+1}) = 0$ for some h ($0 < h < m$),

(2) $g_2(\alpha) = 0$

The degree of $g_1(X)$ is a factor m' of m and the degree of $g_2(X)$ is m. Let

$$h_1(X) = X^{m'} g_1(X^{-1}), \; h_2(X) = X^m g_2(X^{-1}) .$$

Let C_o, C and C' denote binary cyclic codes with length 2^m-1 generated by $g_1(X)g_2(X)$, $(X^{2^m-1}-1)/(h_1(X)h_2(X))$ and $(X^{2^m-1}-1)/[(X-1)h_1(X)h_2(X)]$ respectively. Then C is the dual code of C_o and a subcode of C'. If $h = 1$, then C_o is a double error correcting BCH code, and if m is odd and $h = (m-1)/2$, then C is a BCH code with the second largest t for given m.

In what follows, the weight distribution formula of code C for any m and h will be derived. This problem is closely related to the cross-correlation problem between two different maximum length sequences.* Some applications to the problem will be presented in section 6.

2. Preliminary Lemmas

Lemma 1: The extended code of C' or C_o is invariant under π.

This lemma follows from the definition of C' or C_o and a general theorem [2]. Let

$$m = m'm'' . \quad (1)$$

Since $\alpha^{2^{m-h}+1}$ is a root of $g_1(X)$, it can be assumed that

$$2h \leq m. \quad (2)$$

Since $(2^{m'}-1)(2^h+1)$ is divisible by $(2^m-1) = (2^{m'}-1)(2^{m'(m''-1)} + 2^{m'(m''-2)} + \dots + 1)$,

$$h \geq m'(m''-1) .$$

From (1) and (2),

$$m'm'' \geq 2h \geq 2m'(m''-1) . \quad (3)$$

Hence,

$$m'' = 1 \text{ or } 2.$$

If m'' = 2, then it follows from (3) that

$$m' = h.$$

That is, there are only two cases:

$$m' = m$$

and

$$m' = m/2 = h.$$

* Dr. B. Elspas pointed out this relation.

The following well-known lemmas will be used later.

Lemma 2: Let $u(\ell)$ denote the smallest positive integer u such that $2^u \equiv 1 \pmod{\ell}$. Then, $2^{u'} \equiv 1 \pmod{\ell}$ if and only if $u' \equiv 0 \pmod{u(\ell)}$.

Let (ℓ, ℓ') denote the greatest common divisor of ℓ and ℓ'.

Corollary 3: Let $u = (u_1, u_2)$. Then,

$$2^u - 1 = (2^{u_1} - 1, 2^{u_2} - 1).$$

Lemma 4: 2^u+1 (or 2^u-1) is divisible by $2^{u'}+1$, if and only if u is divisible by u' and u/u' is odd (or even).

Let $c' = (m,h)$, $c = (m,2h)$ and $\nu = (2^m-1, 2^h+1)$. By Corollary 3,

$$2^{c'} - 1 = (2^m - 1, 2^h - 1), \tag{4}$$

$$2^c - 1 = (2^m - 1, 2^{2h} - 1). \tag{5}$$

Since $(2^h+1, 2^h-1) = 1$,

$$(2^m-1, 2^{2h}-1) = (2^m-1, 2^h+1)(2^m-1, 2^h-1).$$

Thus,

$$(2^c-1)/\nu = 2^{c'}-1.$$

By definition, $c = c'$ or $2c'$. Therefore, we have:

Lemma 5: If $c = c'$, then $\nu = 1$. Otherwise,

$$\nu = 2^{c'}+1 = 2^{c/2}+1. \tag{6}$$

The next lemma is due to Pless [3].

Lemma 6: Let a_j and b_j denote the number of code vectors of weight j in a code A and the number of code vectors of weight j in the dual code of A respectively. If $b_1 = b_2 = 0$, then the following power moment identities hold:

$$\Sigma a_j = 2^k$$

$$\Sigma j\, a_j = 2^{k-1}n$$

$$\Sigma j^2 a_j = 2^{k-2}n(n+1)$$

$$\Sigma j^3 a_j = 2^{k-3}(n^3+3n^2) - 3!2^{k-3}b_3$$

$$\Sigma j^4 a_j = 2^{k-4}(n^4+6n^3+3n^2-2n) - 4!2^{k-4}nb_3 + 4!2^{k-4}b_4,$$

where k denotes the number of information digits.

Let C_1 and C_2 denote binary cyclic codes with length 2^m-1 generated by $(X^{2^m-1}-1)/h_1(X)$ and $(X^{2^m-1}-1)/h_2(X)$ respectively. Codes C_1 and C_2 are subcodes of C and C'. If the degree of $g_1(X)$ is m, then the roots of $h_1(X) = X^m g_1(X^{-1})$ are:

$$\alpha^{-(2^h+1)} = \alpha^{2^m-2^h-2},\ \alpha^{-2(2^h+1)} = \alpha^{2^m-2^{h+1}-2-1},\ \dots,$$

$$\alpha^{-2^{m-h-1}(2^h+1)} = \alpha^{2^{m-1}-2^{m-h-1}-1},\ \alpha^{-2^{(m-h)}(2^h+1)} = \alpha^{2^m-2^{m-h}-2},$$

$$\dots,\ \alpha^{-2^{m-1}(2^h+1)} = \alpha^{2^{m-1}-2^{h-1}-1}.$$

There is no i $(0 \leq i < 2^{m-1})$ with $h_1(\alpha^i) = 0$ except for

$$i_1 = 2^{m-1}-2^{m-h-1}-1$$

and

$$i_1' = 2^{m-1}-2^{h-1}-1.$$

By (2), $i_1 < i_1'$.

If $m' = m/2$, then the roots of $h_1(X)$ are:

$$\alpha^{-(2^{m'}+1)} = \alpha^{2^m-2^{m'}-2},\ \alpha^{-2(2^{m'}+1)} = \alpha^{2^m-2^{m'+1}-2-1},\ \dots$$

$$\alpha^{-2^{m'-1}(2^{m'}+1)} = \alpha^{2^{m-1}-2^{m'-1}-1}.$$

there is no i $(0 \le i < 2^{m-1})$ with $h_1(\alpha^i) = 0$ except for

$$i_1 = 2^{m-1}-2^{m'-1}-1.$$

The roots of $h_2(X)$ are $\alpha^{-1} = \alpha^{2^m-2}, \alpha^{-2} = \alpha^{2^m-3}, \ldots, \alpha^{-2^{m-1}} = \alpha^{2^{m-1}-1}$. As it is done above, here we let

$$i_2 = 2^{m-1}-1 .$$

Let $X_1, X_2, \ldots, X_w$ be the location numbers of code vector* $v(x)$ of C'. Then,

$$v(\alpha^i) = \sum_{f=1}^{w} X_f^{\,i} \quad , \quad 0 \le i < 2^m-1$$

For any $\beta_o \in GF(2)$, any $\beta_1 \in GF(2^{m'})$ and any $\beta_2 \in GF(2^m)$, there exists a unique code vector $v(x)$ of C' such that $v(1) = \beta_o$, $v(\alpha^{i_1}) = \beta_1$ and $v(\alpha^{i_2}) = \beta_2$ (Mattson, Solomon [5]). Let $v(\beta_o,\beta_1,\beta_2;x)$ denote the code vector specified by β_o, β_1 and β_2. By definition,

$$x^{\ell} v(\beta_o,\beta_1,\beta_2;x) = v(\beta_o,\alpha^{\ell i_1}\beta_1,\alpha^{\ell i_2}\beta_2;x)$$

If and only if $\beta_o = 0$, $v(\beta_o,\beta_1,\beta_2;x) \in C$. If and only if $\beta_o = \beta_1 = 0$ (or $\beta_o = \beta_2 = 0$), then $v(\beta_o,\beta_1,\beta_2;x) \in C_2$ (or C_1). The cyclic permutations on code word symbols induce a permutation group on the code vectors of C', which divides $C-C_2$ into disjoint sets of transitivity. Since $v = (i_1, 2^m-1)$, each set consists of $(2^m-1)/v$ code vectors. In case of $m' = m$, let $v(0,\alpha^i,\beta_2,x)$ $(0 \le i < v,\ \beta_2 \in GF(2^m))$ represent each set. In case of $m' = m/2$, let $v(0,1,\beta_2;x)$ represent each set.

* A polynomial representation will be used for a code vector [4].

Now, consider the extended code C_{ex} of code C'. Let $\overline{v}(\beta_o,\beta_1,\beta_2)$ denote the vector with an overall parity check added to $v(\beta_o,\beta_1,\beta_2;x)$ as the first digit. By definition $C_{ex} = \{\overline{v}(\beta_o,\beta_1,\beta_2)\,|\,v(\beta_o,\beta_1,\beta_2;x)\in C'\}$. Let $X_1,X_2,\ldots,X_w$ be the location numbers of $\overline{v}(\beta_o,\beta_1,\beta_2)$ and let

$$S_i = \sum_{f=1}^{w} X_f^{\,i} \; , \qquad 0 \leq i < 2^m-1 \tag{7}$$

Then, by definition

$$S_{i_1} = \beta_1 \; , \tag{8}$$

$$S_{i_2} = \beta_2 \; , \tag{9}$$

$$S_i = 0 \;(i \not\equiv i_1 2^{\ell}, i_2 2^{\ell} \pmod{2^m-1}\,,\; 0 \leq \ell < m)$$

Therefore,

$$S_i - 0 \;(i \not\equiv i_1, i_1',\;\; 1 \leq i < 2^{m-1}-1) \tag{10}$$

By Lemma 1, $\tau_{1b}\overline{v}(\beta_o,\beta_1,\beta_2)\in C_{ex}$ for any $b\in GF(2^m)$. Let

$$\tau_{1b}\overline{v}(\beta_o,\beta_1,\beta_2) = \overline{v}(\beta_o',\beta_1',\beta_2') \; . \tag{11}$$

The weights of $\overline{v}(\beta_o,\beta_1,\beta_2)$ and $\overline{v}(\beta_o',\beta_1',\beta_2')$ are the same. By the definition of τ_{1b},

$$\beta_1' = \sum_{f=1}^{w} (X_f+b)^{i_1}$$

$$\beta_2' = \sum_{f=1}^{w} (X_f+b)^{i_2} \; .$$

Hence

$$\beta_1' = \sum_{f=1}^{w} \sum_{i=0}^{i_1} \binom{i_1}{i} X_f^{\,i} b^{\,i_1-i} = \sum_{i=0}^{i_1} \binom{i_1}{i} S_i b^{\,i_1-i} \; .$$

From (8) and (10),

$$\beta_1' = \beta_i \tag{12}$$

Note that $(X_f+b)^{i_2} = (X_f+b)^{2^{m-1}-1} = (X_f^{2^{m-1}}+b^{2^{m-1}})/(X_f+b) = X_f^{2^{m-1}-1} + X_f^{2^{m-1}-2}b + \dots + b^{2^{m-1}-1}$. Then,

$$\beta_2' = \sum_{f=1}^{w} \sum_{i=0}^{2^{m-1}-1} X_f^{i} b^{2^{m-1}-1-i} = \sum_{i=0}^{2^{m-1}-1} S_i b^{2^{m-1}-1-i} \tag{13}$$

Consider the case of $m' = m$. Since $i_1' \equiv 2^h i_1 \pmod{2^m-1}$, $S_{i_1'} = S_{i_1}^{2^h}$. From (8),(9), (10) and (13),

$$\beta_2' = \beta_1 b^{2^{m-1}-1-i_1} + \beta_1^{2^h} b^{2^{m-1}-1-i_1'} + \beta_2 = \beta_1 b^{2^{m-h-1}}$$

$$+ \beta_1^{2^h} b^{2^{h-1}} + \beta_2 . \tag{14}$$

For the case of $m' = m/2$, it follows from (8), (9), (10) and (13) that

$$\beta_2' = \beta_1 b^{2^{h-1}} + \beta_2 . \tag{15}$$

Hereafter we shall consider the case of $m' = m$ except for section 5. For each i $(0 \leq i < \nu)$, $V_i = \{\alpha^i b^{2^{m-h-1}} + \alpha^{i2^h} b^{2^{h-1}} \mid b \in GF(2^m)\}$ forms a subspace of $GF(2^m)$. Let

$$F_i(X) = \alpha^i X^{2^{m-h-1}} + \alpha^{i2^h} X^{2^{h-1}}$$

$$= \alpha^i X^{2^{h-1}} (X^{2^{h-1}(2^{m-2h}-1)} + \alpha^{i(2^h-1)})$$

If $i = 0$, the order of a nonzero root in $GF(2^m)$ of $F_c(X)$ is a factor of $2^{m-2h}-1$. Since $c = (m,2h) = (m,m-2h)$, $2^c-1 = (2^m-1, 2^{m-2h}-1)$. This implies that the roots in $GF(2^m)$ of $F_0(X)$ are in subfield $GF(2^c)$. Conversely, any element in this subfield is a root of $F_0(X)$. Hence, the dimension of V_0 is m-c. Let V_{00} $(=V_0)$, $V_{01}, V_{02}, \ldots, V_{02^c-1}$ be the cosets of $GF(2^m)$ with respect to V_0. Each coset has 2^{m-c} elements.

For $i \neq 0$, assume that α^j is a root of $F_i(X)$. Then,

$$2^{h\cdot i}(2^{m-2h}-1)j = i(2^h-1) \qquad (\text{mod } 2^m-1)$$

$$(1-2^{2h})j \equiv i2^{h+1}(2^h-1) \qquad (\text{mod } 2^m-1)$$

$$-(2^h+1)j \equiv i2^{h+1} \qquad (\text{mod } 2^m-1)$$

Since ν divides both 2^h+1 and 2^m-1, ν must divide i. However, $0 < i < \nu$. Therefore, there is no root in $GF(2^m)$ of $F_i(X)$ except for zero. Consequently, $V_i = GF(2^m)$.

Let $B_{0j} = \{(\alpha^{\ell i_1}, \alpha^{\ell i_2}\beta) \mid 0 \leq \ell < 2^m-1,\ \beta \epsilon V_{0j}\}$ $(0 \leq j \leq 2^c-1)$ and $B_i = \{(\alpha^{i+\ell i_1}, \beta) \mid 0 \leq \ell < 2^m-1,\ \beta \epsilon GF(2^m)\}$ $(0 < i < \nu)$. Then,

$$|B_{0j}| = (2^m-1)2^{m-c}/\nu \qquad (0 \leq j < 2^c)\ , \tag{16}$$

$$|B_i| = (2^m-1)2^m/\nu \qquad (0 < i < \nu)^* \ . \tag{17}$$

It follows from the definition of B_{0j} or B_i that for any (β_1, β_2) and (β_1', β_2') in the same B_{0j} or B_i and for any $\beta_o \epsilon GF(2)$, there exists permutation π_{ab} such that $\pi_{ab}\bar{v}(\beta_o, \beta_1, \beta_2) = \bar{v}(\beta_o', \beta_1', \beta_2')$ and $\beta_o' \epsilon GF(2)$. Therefore, $\bar{v}(\beta_o, \beta_1, \beta_2)$ and $\bar{v}(\beta_o', \beta_1', \beta_2')$ have the same weight w. If β_o (or β_o') is zero,

*|B| means the number of elements of B.

then $v(0,\beta_1,\beta_2;x)$ (or $v(0,\beta_1',\beta_2';x)$) has weight w. If β_o (or β_o') is one, then $v(1,\beta_1,\beta_2;x)$ (or $v(1,\beta_1',\beta_2';x)$) has weight $w-1$ by definition. Since C' contains all one vector $e = (1,1,\ldots,1)$ and $e(\alpha^i) = \sum_{f=0}^{2^m-2} \alpha^{if} = [(\alpha^i)^{2^m-1}-1]/(\alpha^i-1) = 0$ $(0 < i < 2^m-1)$,

$$v(1,\beta_1,\beta_2;x) = v(0,\beta_1,\beta_2;x) + e(x).$$

Hence, if β_o (or β_o') is one, then $v(0,\beta_1,\beta_2;x)$ (or $v(0,\beta_1',\beta_2';x)$) has weight 2^m-w. Therefore, we have Lemma 8.

Lemma 8: For each j (or i) $(0 \leq j < 2^c,\ 0 < i < \nu)$, there is w_{0j} (or w_i) such that for any $(\beta_1,\beta_2)\in B_{0j}$ (or B_i) the weight of $v(0,\beta_1,\beta_2;x)$ is either w_{0j} (or w_i) or 2^m-w_{0j} (or 2^m-w_i).

3. Case I: $(m,h) = (m,2h)$

Hereafter a_w will denote the number of code vectors of weight w in C and b_w will denote the number of code vectors of weight w in C_o.

Lemma 9: For even w,

$$wa_w = (2^m-w)\,a_{2^m-w},$$

$$wb_w = (2^m-w)\,b_{2^m-w}.$$

This lemma follows from a theorem due to Peterson [1] and Lemma 1. Consequently, if the values of w_{0j}'s $(0 \leq j < 2^c)$ and w_i's $(0 < i < \nu)$ are known, the weight distribution of $C-C_2$ is completely determined. Furthermore, any nonzero vector of C_2 has weight 2^{m-1}, because C_2 is a maximum length sequence code.

Lemma 10: $b_1 = b_2 = 0$, $b_3 = (2^{c'-1}-1)(2^m-1)/3$.

<u>Proof</u>: Since C_o is a subcode of Hamming code,

$$b_1 = b_2 = 0.$$

Assume that α^{j_1}, α^{j_2} and α^{j_3} are the location numbers of a code vector of weight 3 in C_o. Then,

$$\alpha^{j_1} + \alpha^{j_2} = \alpha^{j_3} \tag{18}$$

$$\alpha^{j_1(2^h+1)} + \alpha^{j_2(2^h+1)} = \alpha^{j_3(2^h+1)} \tag{19}$$

From (18),

$$\alpha^{j_3(2^h+1)} = (\alpha^{j_1}+\alpha^{j_2})^{2^h+1} = (\alpha^{j_1 2^h}+\alpha^{j_2 2^h})(\alpha^{j_1}+\alpha^{j_2})$$

$$= \alpha^{j_1(2^h+1)} + \alpha^{j_1 2^h}\alpha^{j_2} + \alpha^{j_1}\alpha^{j_2 2^h} + \alpha^{j_2(2^h+1)}$$

By combining with (19),

$$\alpha^{j_1 2^h}\alpha^{j_2} + \alpha^{j_1}\alpha^{j_2 2^h} = 0,$$

$$\alpha^{(j_1-j_2)(2^h-1)} = 1 . \tag{20}$$

Thus,

$$(j_1-j_2)(2^h-1) \equiv 0 \pmod{2^m-1} .$$

If $c' = (m,h) = 1$, then $(2^h-1, 2^m-1) = 1$. Therefore

$$j_1 = j_2 .$$

This is a contradiction, which leads to the conclusion that $b_3 = 0$. If $c' \neq 1$, then $(2^m-1, 2^h-1) = 2^c-1$. Let

$$\mu = (2^m-1)/(2^c-1) . \tag{21}$$

Then,

$$j_1 \equiv j_2 \pmod{\mu}.$$

Let $j_1 = \ell_1\mu+i$ and $j_2 = \ell_2\mu+i$ $(0 \le i < \mu)$. Since $\alpha^{\ell_1\mu} + \alpha^{\ell_2\mu} = \alpha^{\ell_3\mu}$ for some ℓ_3, it follows from (18) that $j_3 = \ell_3\mu+i$. Conversely, for any i $(0 \le i < \mu)$ and for ℓ_1, ℓ_2, and ℓ_3 such that

$$\alpha^{\ell_1\mu} + \alpha^{\ell_2\mu} = \alpha^{\ell_3\mu} \qquad (22)$$

$$0 \le \ell_1,\ell_2,\ell_3 < 2^{c'}-1 \ , \qquad (23)$$

$\alpha^{\ell_1\mu+i}$, $\alpha^{\ell_2\mu+i}$, and $\alpha^{\ell_3\mu+i}$ satisfy (18) and (19). The number of unordered triplets (ℓ_1,ℓ_2,ℓ_3)'s satisfying (22) and (23) is equal to $\binom{2^{c'}-1}{2}/3$. Consequently,

$$b_3 = \mu \binom{2^{c'}-1}{2}/3 = (2^m-1)(2^{c'-1}-1)/3. \qquad \text{Q.E.D.}$$

<u>Lemma 11</u>: Let I_2 and I_4 denote $\sum_{j\neq 0}(j-2^{m-1})^2 a_j$ and $\sum_{j\neq 0}(j-2^{m-1})^4 a_j$ respectively. Then,

$$I_2 = 2^{2m-2}(2^m-1),$$

$$I_4 = 2^{3m+c'-4}(2^m-1) \ .$$

<u>Proof</u>: Note that $k = 2m$. By using the power moment identities of Lemma 6,

$$\begin{aligned} I_2 &= \Sigma\, j^2 a_j - 2^m \Sigma\, j a_j + 2^{2m-2} \sum_{j\neq 0} a_j \\ &= 2^{2m-2}n(n+1) - 2^{3m-1}n + 2^{2m-2}(2^{2m}-1) \\ &= (2^m-1)(2^{3m-2}-2^{3m-1}+2^{3m-2}+2^{2m-2}) \\ &= (2^m-1)2^{2m-2} \end{aligned}$$

$$\begin{aligned}
I_4 &= \Sigma j^4 a_j - 2^{m+1} \Sigma j^3 a_j + 3\cdot 2^{2m-1} \Sigma j^2 a_j - 2^{3m-1} \Sigma j a_j \\
&\quad + 2^{4m-4} \sum_{j\neq 0} a_j \\
&= 2^{2m-4}(n^4+6n^3+3n^2-2n) - 2^{3m-2}(n^3+3n^2) \\
&\quad + 3\cdot 2^{4m-3} n(n+1) - 2^{5m-2} n + 2^{4m-4}(2^{2m}-1) \\
&\quad + 3(2^{3m-1}-2^{2m-1}n) b_3 + 3\cdot 2^{2m-2} b_4 \\
&= n\{2^{2m-4}[(n+1)^3+3(n+1)(n-1)] - 2^{3m-2}[(n+1)^2 + \\
&\qquad n-1] + 3\cdot 2^{4m-3}(n+1) - 2^{5m-2} + 2^{4m-4}(2^m+1)\} \\
&\quad + 3\cdot 2^{2m-1}(b_3+b_4) \\
&= n\{2^{5m-4}-2^{5m-2}+3\cdot 2^{5m-3}-2^{5m-2}+2^{5m-4} \\
&\qquad + 3\cdot 2^{3m-4}(2^m-2) - 2^{3m-2}(2^m-2) + 2^{4m-4}\} \\
&\quad + 3\cdot 2^{2m-1}(b_3+b_4) \\
&= (2^m-1)\, 2^{3m-3} + 3\cdot 2^{2m-1}(b_3+b_4) \qquad (24)
\end{aligned}$$

Since all one vector $(1,1,\ldots,1)$ is in C_o,

$$b_{2^m-4} = b_3 \ .$$

By Lemmas 9 and 10,

$$\begin{aligned}
b_3+b_4 &= b_{2^m-4} + b_4 = 2^{m-2} b_{2^m-4} = 2^{m-2} b_3 \\
&= 2^{m-2}(2^{c'-1}-1)(2^m-1)/3 \ . \qquad (25)
\end{aligned}$$

By substituting the right hand side of (25) into (24),

$$I_4 = (2^m-1)2^{3m+c'-4} \quad . \qquad \text{Q.E.D.}$$

Let j_M be the smallest nonzero integer such that

$$a_{j_M} + a_{2^m-j_M} \neq 0 \; .$$

By the definition of I_2 and I_4,

$$(j_M-2^{m-1})^2 \geq I_4/I_2 = 2^{m+c'-2} \qquad (26)$$

Consider the case where $c = c'$. Then, $\nu = 1$ by Lemma 5. Since all nonzero vectors in C_2 are of weight 2^{m-1}, it follows from Lemma 8 and (16) that $a_j + a_{2^m-j}$ $(j \neq 0, 2^{m-1})$ must be divisible by $2^{m-c'}(2^m-1) = 2^{m-c}(2^m-1)$. Therefore, from (26)

$$I_2 \geq (j_M-2^{m-1})^2(a_{j_M}+a_{2^m-j_M}) \geq 2^{2m-2}(2^m-1) \qquad (27)$$

By Lemma 11 and (27),

$$I_2 = (j_M-2^{m-1})^2(a_{j_M}+a_{2^m-j_M}) = 2^{2m-2}(2^m-1) \; .$$

Consequently,

$$(j_M-2^{m-1})^2 = 2^{m+c'-2} = 2^{m+c-2} \qquad (28)$$

$$a_{j_M} + a_{2^m-j_M} = 2^{m-c}(2^m-1) \qquad (29)$$

$$a_j = 0 \;(j \neq 0,\, j_M,\, 2^{m-1},\, 2^m-j_M) \, .$$

Hence,

$$j_M = 2^{m-1} - 2^{(m+c)/2-1} \tag{30}$$

$$a_{2^{m-1}} = 2^{2m}-1 - (a_{j_M} + a_{2^m-j_M})$$

$$= (2^m-2^{m-c}+1)(2^m-1)$$

By Lemma 9, (29) and (30),

$$a_{j_M} = (2^{m-c-1}+2^{(m-c)/2-1})(2^m-1)$$

$$a_{2^m-j_M} = (2^{m-c-1}-2^{(m-c)/2-1})(2^m-1)$$

Thus, we have the following theorem.

Theorem 1: If $(m,h) = (m,2h) = c$, then

$$a_0 = 1$$

$$a_{2^{m-1}-2^{(m+c)/2-1}} = (2^{m-c-1}+2^{(m-c)/2-1})(2^m-1)$$

$$a_{2^{m-1}} = (2^m-2^{m-c}+1)(2^m-1)$$

$$a_{2^{m-1}+2^{(m+c)/2-1}} = (2^{m-c-1}-2^{(m-c)/2-1})(2^m-1)$$

$a_j = 0$ for other j.

4. Case II: $2(m,h) = (m,2h) \neq m$

Consider the case in which $2(m,h) = (m,2h)$. Then, $\nu = 2^{c'}+1$ by Lemma 5. Since $v(0,\beta_1,0,x)$ is in C_1, $w_{00} = w_0, w_1, \ldots, w_{\nu-1}$ can be found from the weight distribution of C_1. Each code vector of C_1 is a ν concatenation of a code vector in cyclic code C_1' of length $(2^m-1)/\nu$ which is generated by $(X^{(2^m-1)/\nu}-1)/h_1(X)$. Let $v'(\beta;x)$ denote a code vector $v'(x)$

in C_1' such that $v'(\alpha^{i_1}) = \beta$. With the same argument as the one of section 3, set $C_{1i}' = \{v(\alpha^{i+\ell\nu};x) \mid 0 \leq \ell < (2^m-1)/\nu\}$ $(0 \leq i < \nu)$ consists of $(2^m-1)/\nu$ vectors of the same weight w_i'. Since $v(0,\beta,0;x) = \underbrace{(v'(\beta;x), v'(\beta;x), \ldots, v'(\beta;x))}_{\nu}$, w_i can be given by the following equation:

$$w_i = \nu w_i' . \quad (0 \leq i < \nu)$$

Therefore, by applying Lemma 6 to code C_1', we have

$$(2^m-1)/\nu \sum_{i=0}^{\nu-1} w_i/\nu = 2^{m-1}(2^m-1)/\nu ,$$

$$(2^m-1)/\nu \sum_{i=0}^{\nu-1} (w_i/\nu)^2 = 2^{m-2}(2^m-1)(2^m-1+\nu)/\nu^2 .$$

Thus,

$$\sum_{i=0}^{\nu-1} w_i = \nu 2^{m-1} \tag{31}$$

$$\sum_{i=0}^{\nu-1} w_i^2 = \nu 2^{m-2}(2^m-1+\nu) = \nu 2^{m-2}(2^m+2^{c'}) \tag{32}$$

Therefore,

$$\sum_{i=0}^{\nu-1} (w_i-2^{m-1})^2 = \nu 2^{m-2}(2^m-1+\nu) - 2^m \nu 2^{m-1} + 2^{2m-2}\nu$$

$$= \nu 2^{m-2}(\nu-1) = \nu 2^{m+c'-2} \tag{33}$$

On the other hand, it follows from Lemma 8, (16), (17) and the oefinition of I_2 that

$$I_2 = I_{20} + I_{21},$$

$$I_{20} = 2^{m-c}(2^m-1) \sum_{j=1}^{2^c-1} (w_{0j}-2^{m-1})^2/\nu, \tag{34}$$

$$I_{21} = 2^{m-c}(2^m-1)(w_0-2^{m-1})^2/\nu + 2^m(2^m-1)\sum_{i=1}^{\nu-1} (w_i-2^{m-1})^2/\nu.$$

By Lemma 11 and (33),

$$\begin{aligned} I_2 &= 2^{2m-2}(2^m-1) \\ &\geq I_{21} = 2^{2m+c'-2}(2^m-1) - (2^m-1)(2^m-2^{m-c})(w_0-2^{m-1})^2/\nu. \end{aligned} \tag{35}$$

By a simple calculation,

$$\begin{aligned} (w_0-2^{m-1})^2 &\geq 2^{2m-2}(2^{c'}-1)\nu/(2^m-2^{m-c}) \\ &= 2^{m+c-2} \qquad \text{(by (6))}. \end{aligned}$$

Hence,

$$w_o = 2^{m-1} \pm (2^{(m+c)/2-1} + \delta), \quad \delta \geq 0 \tag{36}$$

Now, by (31) and (32)

$$\begin{aligned} I_2' &= \sum_{i=0}^{\nu-1} (w_i-(2^{m-1} \mp 2^{m/2-1}))^2 \\ &= \nu 2^{m-2}(2^m-1+\nu)-2(2^{m-1}\mp 2^{m/2-1})\nu 2^{m-1}+(2^{m-1}\mp 2^{m/2-1})^2\nu \\ &= \nu\{2^{2m-2}+2^{m+c'-2}-2^{2m-1}\pm 2^{3m/2-1}+2^{2m-2}\mp 2^{3m/2-1}+2^{m-2}\} \\ &= 2^{m-2}(2^{c'}+1)^2 \end{aligned} \tag{37}$$

On the other hand,

$$\begin{aligned} I_2' \geq (w_0-(2^{m-1}\mp 2^{m/2-1}))^2 &= [2^{m-1}\pm(2^{(m+c)/2-1}+\delta)-2^{m-1}\pm 2^{m/2-1}]^2 \\ &= 2^{m-2}(2^{c'}+1+\delta 2^{1-m/2})^2 \end{aligned} \tag{38}$$

From (35), (36), and (37), we have that

$$\delta = 0$$

$$w_0 = 2^{m-1} \pm 2^{(m+c)/2-1} \tag{39}$$

$$w_i = 2^{m-1} \mp 2^{m/2-1} \qquad (0 < i < \nu) \tag{40}$$

Since w_i $(0 \leq i < \nu)$ is divisible by ν, the $\pm$ sign is determined by Lemma 4. Thus, we have:

Theorem 2: Let $a'_{j\nu}$ denote the number of code vectors of weight j in C'_1. If m/c is odd (or even), then

$$a'_0 = 1$$

$$a'_{2^{m-1}-2^{(m+c)/2-1}} \text{ (or } a'_{2^{m-1}+2^{(m+c)/2-1}}) = (2^m-1)/(2^{c/2}+1)$$

$$a'_{2^{m-1}+2^{m/2-1}} \text{ (or } a'_{2^{m-1}-2^{m/2-1}}) = 2^{c/2}(2^m-1)/(2^{c/2}+1).$$

$$a'_j = 0 \quad \text{for other } j.$$

From (35) and (39) it follows that

$$\begin{aligned} I_{21} &= 2^{2m+c'-2}(2^m-1) - (2^m-1)(2^m-2^{m-c})2^{m+c-2}/\nu \\ &= 2^{2m-2}(2^m-1)(2^{c'}-(2^c-1)/\nu) \\ &= 2^{2m-2}(2^m-1) \\ &= I_2 \qquad\qquad \text{(by (35))}. \end{aligned}$$

By (34),

$$I_{20} = (2^m-1)2^{m-c}/\nu \sum_{j=1}^{2^c-1} (w_{0j}-2^{m-1})^2 = 0$$

Hence,

$$w_{0j} = 2^{m-1} \qquad (1 \leq j < 2^c). \tag{41}$$

By (16), (17), Lemma 8, (39), (40) and (41), we have:

$$a_{2^{m-1}-2^{m/2-1}} + a_{2^{m-1}+2^{m/2-1}} = (2^m-1)2^{m+c/2}/(2^{c/2}+1)$$

$$a_{2^{m-1}} = (2^m-1)2^{m-c}(2^c-1)/(2^{c/2}+1) + 2^m-1$$

$$a_{2^{m-1}-2^{(m+c)/2-1}} + a_{2^{m-1}+2^{(m+c)/2-1}} = (2^m-1)2^{m-c}/(2^{c/2}+1)$$

Thus, the next theorem follows from Lemma 9.

Theorem 3: If $2(m,h) = (m,2h) = c$ and $c \neq m$, then

$$a_0 = 1$$

$$a_{2^{m-1}-2^{(m+c)/2-1}} = (2^m-1)(2^{(m-c)/2}+1)2^{(m-c)/2-1}/(2^{c/2}+1)$$

$$a_{2^{m-1}-2^{m/2}} = (2^m-1)(2^{m/2}+1)2^{(m+c)/2-1}/(2^{c/2}+1)$$

$$a_{2^{m-1}} = (2^m-1)((2^{c/2}-1)2^{m-c}+1)$$

$$a_{2^{m-1}+2^{m/2}} = (2^m-1)(2^{m/2}-1)2^{(m+c)/2-1}/(2^{c/2}+1)$$

$$a_{2^{m-1}+2^{(m+c)/2-1}} = (2^m-1)(2^{(m-c)/2}-1)2^{(m-c)/2-1}/(2^{c/2}+1)$$

$$a_j = 0 \quad \text{for other } j.$$

5. Case III: $2(m,h) = (m,2h) = m$

Consider the case of $m = 2h$. For any $\beta_1 \neq 0$, β_2 in $GF(2^m)$, there exists $b \in GF(2^m)$ such that

$$\beta_1 b^{2^{h-1}} + \beta_2 = 0 ,$$

because $(2^{h-1}, 2^m-1) = 1$. From (15) and a similar argument to the one for the case of $m = m'$, it follows that there exists w such that the weight of any code vector in $C-C_2$ is either w or 2^m-w. Since C_1', the cyclic code of length $2^{m/2}-1$ generated by $(X^{2^{m/2}-1}-1)/g_1(X)$, is a maximum length sequence code, C_1 consists of one zero vector and $2^{m/2}-1$ vectors of weight $2^{m/2-1}$ $(2^{m/2}+1)$. Therefore,

$$w = (2^{m/2}+1)\,2^{m/2-1}.$$

On the other hand, C_2 is a maximum length sequence code of length 2^m-1. Hence,

$$a_{2^{m-1}} = 2^m-1 \;.$$

According to Lemma 9, we have:

Theorem 4: If m = 2h, then

$$a_0 = 1$$

$$a_{2^{m-1}-2^{m/2-1}} = (2^{m/2}-1)(2^{m-1}+2^{m/2-1})$$

$$a_{2^{m-1}} = 2^m-1$$

$$a_{2^{m-1}+2^{m/2-1}} = (2^{m/2}-1)(2^{m-1}-2^{m/2-1})$$

$$a_j = 0 \qquad \text{for other } j.$$

6. Crosscorrelation Functions of Two Maximum Length Sequences

It follows from Lemma 5 that α^{2^h+1} is a primitive element if and only if c = c'. Assume that c = c'. Let

$$v(0,1,0;x) = \sum_{f=0}^{2^m-2} v_{1f}x^f$$

$$v(0,0,1;x) = \sum_{f=0}^{2^m-2} v_{2f}x^f \;.$$

Then, $v_1 = v_{10},v_{11},\ldots,v_{12^m-2}$ and $v_2 = v_{20},v_{21},\ldots,v_{22^m-2}$ are maximum length sequences of length 2^m-1. In v_1 and v_2, replace 0 by -1. Let $u_1 = u_{10},u_{11},\ldots,u_{12^m-2}$ and $u_2 = u_{20},u_{21},\ldots,u_{22^m-2}$ be the resulting sequences of real numbers 1 and -1. Correlation function $\theta(j)$ of u_1 and u_2 is defined by

$$\theta(j) = \sum_{f=0}^{2^m-2} u_{1f}u_{2f-j} ,$$

where suffix $f - j$ is to be taken mod 2^m-1. Note that

$$v(0,1,0;x) + x^j v(0,0,1;x) = v(0,1,\alpha^{ji_2};x) .$$

If $v(0,1,\alpha^{ji_2};x)$ has weight w, then

$$\theta(j) = 2^m-1-2w . \tag{42}$$

Let s_i denote the number of j's $(0 \le j < 2^m-1)$ with $\theta(j) = i$. Then, s_i is the number of vectors $v(0,1,\beta;x)$ with weight $(2^m-1-i)/2$. From sections 2 and 3, we have theorem 5.

Theorem 5:

$$s_{-2^{(m+c)/2}-1} = 2^{m-c-1}-2^{(m-c)/2-1} ,$$

$$s_{-1} = 2^m-2^{m-c} ,$$

$$s_{2^{(m+c)/2}-1} = 2^{m-c-1} + 2^{(m-c)/2-1} ,$$

$$s_i = 0 \quad \text{for other } i.$$

For $0 \le j < 2^m-1$, let

$$\theta_j = 1 \text{ if } \theta(j) = -2^{(m+c)/2}-1 \text{ or } 2^{(m+c)/2}-1 ,$$

$$\theta_j = 0 \quad \text{if } \theta(j) = -1.$$

Sequence $\theta = \theta_0,\theta_1,\ldots,\theta_{2^m-2}$ will be called the correlation sequence of u_1 and u_2. We shall characterize the correlation sequence below. Recall that

$$V_0 = V_{00} = \{b^{2^{m-h-1}} + b^{2^{h-1}} | b \in GF(2^m)\}$$

Since $(2^{h-1}, 2^m-1) = 1$,

$$V_{00} = \{b^{2^{m-2h}} + b | b \in GF(2^m)\}$$

Since $(m-2h, m) = c$, the Galois group of $GF(2^m)$ over $GF(2^c)$ is generated by the automorphism $X \rightarrow X^{2^{m-2h}}$ (by Theorem 9, p. 127 of [6]). Therefore, from the trace theorem (p. 121 of [6]) it follows that

$$V_{00} = \{b | \sigma(b) = 0,\ b \in GF(2^m)\},$$

where $\sigma(b)$ denotes the trace of b in $GF(2^m)$ over $GF(2^c)$, and

$$\sigma(b) = b + b^{2^c} + b^{2^{2c}} + \ldots + b^{2^{m-c}} .$$

Hence, any element of each coset V_{0j} has the same trace $t_j \in GF(2^c)$, and if $j \neq j'$, $t_j \neq t_{j'}$.

Note that $v^2(0,\beta_1,\beta_2;x) = v(0,\beta_1,\beta_2;x^2) = v(0,\beta_1^2,\beta_2^2;x) \in C$ and that $v(0,\beta_1,\beta_2;x)$ and $v(0,\beta_1,\beta_2;x^2)$ have the same weight. Consequently, if $t_{j'} = t_j^2$, then $w_{0j'} = w_{0j}$. From the proof of Theorem 1 it follows that there is only one j_0 such that

$$w_{0j_0} = 2^{m-1} - 2^{(m+c)/2-1}$$

$$w_{0j} = 2^{m-1},\ j \neq j_0 .$$

Since $t_{j_0} = t_{j_0}^2$, $t_{j_0} = 0$ or 1. Since C_1 is a maximum length sequence code, w_{00} must be 2^{m-1}. Therefore, $t_{j_0} = 1$. This implies that the weight of $v(0,1,\beta;x)$ is not equal to 2^{m-1} if and only if $\beta + \beta^{2^c} + \beta^{2^{2c}} + \ldots + \beta^{2^{m-c}} = 1$. From (42), $\theta(j) \neq -1$, if and only if $\alpha^{ji_2} + \alpha^{ji_2 2^c} + \alpha^{ji_2 2^{2c}} + \ldots + \alpha^{ji_2 2^{m-c}} = 1$. Since $\alpha^{2i_2} = \alpha^{2^m-2} = \alpha^{-1}$ and $\alpha^{-2^{m-1}} = \alpha^{i_2}$, we have Theorem 6.

Theorem 6: $\theta_j = 1$ if and only if $\alpha^{-j} + \alpha^{-j2^c} + \alpha^{-j2^{2c}} + \ldots + \alpha^{-j2^{m-c}} = 1$.

Now consider the case of $c = 1$. By definition, $v(0,0,1;\alpha^{i_2}) = 1$. Therefore,

$$v(0,0,1;\alpha^{-2^\ell}) = 1 \qquad (0 \leq \ell < m) \ .$$

On the other hand, for any $\alpha^j \neq \alpha^{-2^\ell}$ $(0 \leq \ell < m)$,

$$v(0,0,1;\alpha^j) = 0 \ .$$

By the formula due to Reed and Solomon [7],

$$v_{2f} = \sum_{j=0}^{2^m-2} v(0,0,1;\alpha^j)\alpha^{-jf}$$

$$= \alpha^f + \alpha^{2f} + \alpha^{2^2f} + \ldots + \alpha^{2^{m-1}f} \ .$$

Hence, by Theorem 6

$$\theta_j = v_{22^m-1-j} \ .$$

This implies the following corollary.

Corollary 7: If $(m,h) = (m,2h) = 1$, then the correlation sequence of the maximum length sequence generated by $h_1(X)$ and the one generated by $h_2(X)$ is the maximum length sequence generated by $g_2(X) = X^m h_2(X^{-1})$.

R. Gold and E. Kopitzka [8] observed that for some pairs of maximum length sequences the correlation sequences are also maximum length sequences and they listed all such pairs of sequences of length 8191 or less. Among 28 listed pairs, 25 cases are covered by Corollary 7.

Acknowledgment

The author is grateful to Professors W. W. Peterson, R. T. Chien and J. S. Lin for many valuable suggestions and to Professors M. E. Van Valkenburg and H. Ozaki for their support.

References

1. Peterson, W. W., "On the Weight Structure and Symmetry of BCH Codes," Report of University of Hawaii, Contract No. AF19(628)-4379, No. 1, (July, 1965).

2. Kasami, T., "Some Invariant Properties of BCH Codes and RM Codes," Seminar Note of CSL, University of Illinois, (March, 1966). A full paper is being prepared jointly with W. W. Peterson and S. J. Lin.

3. Pless, V., "Power Moment Identities on Weight Distributions in Error Correcting Codes," *Information and Control*, *6*, 147-152 (1963).

4. Peterson, W. W., *Error Correcting Codes*, Wiley, New York (1961).

5. Mattson, H. F. and Solomon, G., "A New Treatment of Bose-Chaudhuri Codes," *J. Soc. Indust. Appl. Math.*, *9*, No. 4, (December, 1961).

6. Reed, I. S. and Solomon, G., "Decoding Procedure for a Polynomial Code," Group Report 47,24, Lincoln Laboratory, (1959).

7. Albert, A. A., *Fundamental Concepts of Higher Algebra*, The University of Chicago Press, (1956).

8. Gold, R. and Kopitzka, E., "Study of Correlation Properties of Binary Sequences Vol. 1 ~ 5," Reports of Magnovon Research Laboratories, (August, 1965).

DOCUMENT CONTROL DATA R&D

(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)

1. ORIGINATING ACTIVITY (Corporate author) University of Illinois Coordinated Science Laboratory Urbana, Illinois 61801	2a. REPORT SECURITY CLASSIFICATION Unclassified 2b. GROUP

3. REPORT TITLE

WEIGHT DISTRIBUTION FORMULA FOR SOME CLASS OF CYCLIC CODES

4. DESCRIPTIVE NOTES (Type of report and inclusive dates)

5. AUTHOR(S) (Last name, first name, initial)

Kasami, Tadao

6. REPORT DATE April, 1966	7a. TOTAL NO. OF PAGES 24	7b. NO. OF REFS. 8

8a. CONTRACT OR GRANT NO. DA 28 043 AMC 00073(E) b. PROJECT NO. 20014501B31F c. Also National Science Foundation Grant NSF GK-690 d.	9a. ORIGINATOR'S REPORT NUMBER(S) R-285 9b. OTHER REPORT NO(S) (Any other numbers that may be assigned this report)

10. AVAILABILITY/LIMITATION NOTICES

Distribution of this report is unlimited.

11. SUPPLEMENTARY NOTES	12. SPONSORING MILITARY ACTIVITY Joint Services Electronics Program thru U. S. Army Electronics Command Ft. Monmouth, New Jersey 07703

13. ABSTRACT

Let $h_1(X)$ and $h_2(X)$ be different irreducible polynomials such that $h_1(\alpha^{-2^h-1}) = 0$ for some $h(0 < h < m)$ and $h_2(\alpha^{-1}) = 0$, α being a primitive element of $GF(2^m)$ This paper presents the weight distribution formula of the code of length 2^m-1 generated by $(X^{2^m-1} - 1)/(h_1(X)h_2(X))$ for any m and h. Some applications to the cross-correlation problem between two different maximum length sequences are presented.

Security Classification

KEY WORDS	LINK A		LINK B		LINK C	
	ROLE	WT	ROLE	WT	ROLE	WT
weight distribution cyclic codes cross-correlation maximum length sequences						

INSTRUCTIONS

[illegible] ACTIVITY: [illegible] the [illegible] Department [illegible] Defense [illegible] report.

[illegible] REPORT SECURITY CLASSIFICATION: [illegible] security classification of the report. [illegible] whether "Restricted Data" [illegible] be in accordance [illegible]

[illegible] that optional [illegible]

[illegible] report title in all [illegible] unclassified, [illegible]

[illegible] NOTES: If appropriate, enter the type of report, [illegible] progress, [illegible] annual, or final. [illegible] reporting period is covered.

[illegible] AUTHOR(S): Enter the name(s) of author(s) as shown on [illegible] report. Enter last name, first name, middle initial. [illegible] rank and branch of service. The name of [illegible] author is an absolute minimum requirement.

[illegible] DATE: Enter the date of the report as day, month, [illegible] month, year. If more than one date appears on the [illegible] date of publication.

[illegible] NUMBER OF PAGES: The total page count should follow [illegible] pagination procedures, i.e., enter the number of [illegible] information.

[illegible] NUMBER OF REFERENCES: Enter the total number of references cited in the report.

[illegible] CONTRACT OR GRANT NUMBER: If appropriate, enter the [illegible] the contract or grant under which the [illegible] written.

[illegible] PROJECT NUMBER: Enter the appropriate military [illegible] identification, such as project number, subproject number, [illegible] numbers, task number, etc.

[illegible] ORIGINATOR'S REPORT NUMBER(S): Enter the official report [illegible] which the document will be identified and controlled by the originating activity. This number must be [illegible] to this report.

9b. OTHER REPORT NUMBER(S): If the report has been assigned [illegible] other report numbers (either by the originator or by the [illegible]), also enter this number(s).

[illegible] AVAILABILITY/LIMITATION NOTICES: [illegible]

(1) "[illegible] report [illegible] DDC."

(2) "[illegible] report by DDC is not authorized."

(3) "[illegible] this report directly from DDC. Other [illegible] shall request through

_______________________________."

(4) "[illegible] this report [illegible] shall request through

_______________________________."

(5) "[illegible]

_______________________________."

[illegible] report [illegible] Office of [illegible] Department of [illegible] price, if known.

11. SUPPLEMENTARY NOTES: Use for additional explanatory notes.

12. SPONSORING MILITARY ACTIVITY: Enter the name of the departmental project office or laboratory sponsoring (paying for) the research and development. Include address.

13. ABSTRACT: Enter an abstract giving a brief and factual summary of the document indicative of the report, even though it may also appear elsewhere in the body of the technical report. If additional space is required, a continuation sheet shall be attached.

It is highly desirable that the abstract of classified reports be unclassified. Each paragraph of the abstract shall end with an indication of the military security classification of the information in the paragraph, represented as (TS), (S), (C), or (U).

There is no limitation on the length of the abstract. However, the suggested length is from 150 to 225 words.

14. KEY WORDS: Key words are technically meaningful terms or short phrases that characterize a report and may be used as index entries for cataloging the report. Key words must be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location, may be used as key words but will be followed by an indication of technical context. The assignment of links, roles, and weights is optional.

DD FORM 1 JAN 64 1473

Best Available Copy

Security Classification